

09/965, 455



日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日  
Date of Application:

2000年 9月29日

出 願 番 号  
Application Number:

特願2000-297937

出 願 人  
Applicant(s):

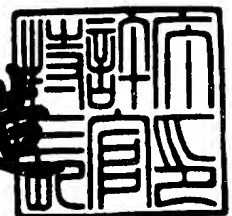
株式会社日立製作所

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 9月18日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3085771

【書類名】 特許願

【整理番号】 K00015381

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00

【発明者】

    【住所又は居所】 東京都江東区新砂一丁目 6 番 2 7 号 株式会社日立製作所 公共システム事業部内

    【氏名】 斎藤 司

【発明者】

    【住所又は居所】 東京都江東区新砂一丁目 6 番 2 7 号 株式会社日立製作所 公共システム事業部内

    【氏名】 三浦 信治

【発明者】

    【住所又は居所】 東京都江東区新砂一丁目 6 番 2 7 号 株式会社日立製作所 公共システム事業部内

    【氏名】 村上 剛司

【特許出願人】

    【識別番号】 000005108

    【氏名又は名称】 株式会社日立製作所

【代理人】

    【識別番号】 100083552

    【弁理士】

    【氏名又は名称】 秋田 収喜

    【電話番号】 03-3893-6221

【手数料の表示】

    【予納台帳番号】 014579

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

【物件名】 図面 1  
【物件名】 要約書 1  
【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 アクセス制御方法及びその実施装置並びにその処理プログラムを記録した記録媒体

【特許請求の範囲】

【請求項 1】 利用者から受付けたアクセス内容の実行を制御するアクセス制御方法において、

利用者から要求されたアクセスの内容を示すアクセス内容を受付けるステップと、前記受付けたアクセス内容の実行を当該利用者の利用者属性と共に要求するステップと、前記要求されたアクセス内容の処理をそのアクセス内容と共に送られた利用者属性に対応する範囲内で実行するステップとを有することを特徴とするアクセス制御方法。

【請求項 2】 前記利用者属性の開示内容を利用者属性開示ポリシーに従って制限することを特徴とする請求項 1 に記載されたアクセス制御方法。

【請求項 3】 前記利用者属性の開示先を利用者属性開示ポリシーに従って制限することを特徴とする請求項 1 または請求項 2 のいずれかに記載されたアクセス制御方法。

【請求項 4】 利用者から受付けたアクセス内容の実行を制御するアクセス制御システムにおいて、

利用者から要求されたアクセスの内容を示すアクセス内容を受付けるアクセス依頼処理部と、前記受付けたアクセス内容の実行を当該利用者の利用者属性と共に要求するアクセス要求処理部と、前記要求されたアクセス内容の処理をそのアクセス内容と共に送られた利用者属性に対応する範囲内で実行するアクセス実行処理部とを備えることを特徴とするアクセス制御システム。

【請求項 5】 利用者から受付けたアクセス内容の実行を制御するアクセス制御システムとしてコンピュータを機能させる為のプログラムを記録したコンピュータ読み取り可能な記録媒体において、

利用者から要求されたアクセスの内容を示すアクセス内容を受付けるアクセス依頼処理部と、前記受付けたアクセス内容の実行を当該利用者の利用者属性と共に要求するアクセス要求処理部と、前記要求されたアクセス内容の処理をそのア

クセス内容と共に送られた利用者属性に対応する範囲内で実行するアクセス実行処理部としてコンピュータを機能させる為のプログラムを記録したことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は利用者から受付けたアクセス内容の実行を制御するアクセス制御システムに関し、特に利用者から受付けた情報要求内容の検索をその利用者の利用者属性に応じて制御するアクセス制御システムに適用して有効な技術に関するものである。

【0002】

【従来技術】

従来、インターネット上のサイトでは各種情報の発信が行われており、それらのサイトへアクセスすることにより、誰でもが多くの情報を参照することができる。この様なインターネット上で情報を発信しようとする場合には、インターネット上でサイトを開設し、発信しようとする情報が書き込まれたHTML (Hyper Text Markup Language)等のファイルを作成しておき、誰でもがその情報を読み出せる様にそのファイルへのアクセス権限を設定しておけば良い。

【0003】

この様にして不特定多数の利用者に対して発信されている情報を参照しようとする場合、利用者は、インターネット上の検索サイトを利用して特定のキーワードを含むサイトを検索したり、他のサイトに設けられているリンクを辿ったりして目的のサイトに遷移し、そのサイトから発信されている情報を参照することができる。例えば、ある利用者がインフルエンザに関する情報を収集しようとする際には、検索サイトでキーワード「インフルエンザ」を入力して検索を行うことにより、単語「インフルエンザ」を含む情報を開示しているサイトを検索することができる。

【0004】

また、情報を発信しているサイトへのアクセスに制限を設け、特定の利用者だ

けにそのサイトの情報を開示する場合もある。この様なアクセス制限では、予め特定の利用者に対してユーザ登録を行ってユーザIDとパスワードを発行しておき、そのユーザID及びパスワードを入力した特定の利用者のみにその情報へのアクセスを許可する等の方法が用いられている。

#### 【0005】

なお特定の権限を持つ人だけに文書やプログラムなどの利用を許可したり、インターネット上で提供するサービスにおいて、会員の持つ資格によって利用できるサービスや閲覧できる情報の内容を切り換えることが可能なアクセス制御方法及びシステム及びアクセス制御プログラムを格納した記憶媒体については特開平10-320288号公報に記載されている。その概要は、個々の利用者を区別するための利用者識別情報と該利用者の分類情報を保持し、あるオブジェクトがどの範囲の利用者から利用可能かを表す利用範囲情報とオブジェクト本体を一体的に格納し、利用者がオブジェクトを要求すると、利用者の要求するオブジェクトが該利用者から利用可能かどうかを、利用者識別情報、利用者の分類情報及び、利用範囲情報を参照して判定し個々のオブジェクト毎に利用範囲情報に対応する利用者のみにオブジェクトの利用を許可し、オブジェクトを提供するものである。

#### 【0006】

##### 【発明が解決しようとする課題】

前記従来技術において、任意の利用者からのアクセスを許可しているインターネット上のサイトでは、アクセスしているのがどういった利用者であるかに関わらず同様の処理が行われる為、利用者が望む結果が得られない場合が生じるという問題がある。

#### 【0007】

例えば、ある利用者がインフルエンザに関する情報を収集しようとする際には、一般の人がインフルエンザとはどういうものであるかを知りたい場合や、医師が最新のウィルス種別及び対応ワクチンについて調査したい場合等、その利用者によって必要とする情報の内容が異なってくるが、検索サイトで「インフルエンザ」を検索した場合には、利用者がどういった人間であるかに関わらず、キーワ

ード「インフルエンザ」を含む全てのサイトが検索される為、利用者は、それらの多くのサイトの情報の中から自分の望む情報がどれであるかを探さなければならない。

【0008】

前記従来の様に利用者が望む結果が得られない場合には、利用者毎に木目細かなアクセス制御を行うことが望まれるが、前記の様なインターネット上のアクセスでは、不特定の利用者が不特定のサイトへアクセスすることが多い為、ユーザID及びパスワード等によるユーザ管理ではそのユーザ管理に必要な負担が増大するという問題がある。

【0009】

すなわち前記従来の技術において、ユーザID及びパスワード等によって利用者毎に異なるアクセス制御を行おうとした場合、利用者は目的とする情報が得られそうな全てのサイトで予めユーザID及びパスワードを取得して管理し、またサイト運営者はアクセスを希望する全ての利用者毎に異なるアクセス権限を設定して管理する必要がある為、不特定多数の利用者が不特定多数のサイトへアクセスすることを想定した場合では、管理対象のユーザID及びパスワードの数が増大し、それらを管理することが実質的に不可能になるという問題がある。

【0010】

本発明の目的は上記問題を解決し、要求されたアクセス内容の実行側での利用者管理等の負担を増やすことなく利用者毎に木目細かなアクセス制御を行うことが可能な技術を提供することにある。

【0011】

【課題を解決するための手段】

本発明は、利用者から受付けたアクセス内容の実行を制御するアクセス制御システムにおいて、利用者が要求したアクセス内容の実行を当該利用者の利用者属性に応じて制御するものである。

【0012】

本発明のアクセス制御システムでは、まず利用者の各種属性を示す利用者属性をプロバイダ側処理装置に設定しておき、利用者から受付けたアクセス内容の実

行を行うアクセス処理装置に当該利用者の利用者属性に応じたアクセス制御を行う為の情報を設定しておく。

【0013】

利用者側処理装置では、利用者から要求された情報検索等のアクセスの内容を示すアクセス内容を受付けて、当該利用者の利用者属性の開示方針を示す利用者属性開示ポリシーと共にプロバイダ側処理装置に送る。

【0014】

プロバイダ側処理装置では、前記受付けたアクセス内容の処理を実行するアクセス処理装置を利用者属性開示ポリシーに従って決定し、前記利用者属性の開示先の制限を行う。またプロバイダ側処理装置では、前記決定したアクセス処理装置に対して開示する利用者属性の内容を利用者属性開示ポリシーに従って決定し、前記利用者属性の開示内容の制限を行う。そして前記受付けたアクセス内容及び前記制限した開示内容の利用者属性を前記決定したアクセス処理装置に送り、そのアクセス内容の実行を要求する。

【0015】

アクセス処理装置では、アクセス内容と共に送られた利用者属性に応じてアクセス制御レベルを設定し、前記要求されたアクセス内容の処理をそのアクセス制御レベルに対応した範囲内で実行する。

【0016】

以上の様に本発明のアクセス制御システムによれば、利用者から要求されたアクセス内容の実行を当該利用者の利用者属性に応じて制御するので、要求されたアクセス内容の実行側での利用者管理等の負担を増やすことなく利用者毎に木目細かなアクセス制御を行うことが可能である。

【0017】

【発明の実施の形態】

以下に利用者から受付けたアクセス内容の実行をその利用者の属性情報に応じて制御する一実施形態のアクセス制御システムについて説明する。

【0018】

図1は本実施形態のアクセス制御システムの概略構成を示す図である。図1に



示す様に本実施形態のアクセス制御システムは、プロバイダ側処理装置 1 0 0 と、利用者側処理装置 1 0 1 と、アクセス処理装置 1 0 2 とを有している。

#### 【 0 0 1 9 】

プロバイダ側処理装置 1 0 0 は、利用者から要求されたアクセスの内容を示すアクセス内容と当該利用者の利用者属性の開示方針を示す利用者属性開示ポリシーを利用者側処理装置 1 0 1 から受付け、当該利用者属性開示ポリシーに従って決定したアクセス処理装置 1 0 2 に当該アクセス内容の処理を要求するプロバイダ側の情報処理装置である。

#### 【 0 0 2 0 】

利用者側処理装置 1 0 1 は、アクセス内容及び利用者属性開示ポリシーを利用者から受付けて当該アクセス内容の処理をプロバイダ側処理装置 1 0 0 に依頼する利用者側の情報処理装置である。アクセス処理装置 1 0 2 は、プロバイダ側処理装置 1 0 0 から要求されたアクセス内容の処理をそのアクセス内容と共に送られた利用者属性に対応する範囲内で実行する情報処理装置である。

#### 【 0 0 2 1 】

図 2 は本実施形態のプロバイダ側処理装置 1 0 0 の概略構成を示す図である。図 2 に示す様に本実施形態のプロバイダ側処理装置 1 0 0 は、CPU 2 0 1 と、メモリ 2 0 2 と、磁気ディスク装置 2 0 3 と、入力装置 2 0 4 と、出力装置 2 0 5 と、CD-ROM 装置 2 0 6 と、利用者属性 DB 2 0 7 とを有している。

#### 【 0 0 2 2 】

CPU 2 0 1 は、プロバイダ側処理装置 1 0 0 全体の動作を制御する装置である。メモリ 2 0 2 は、プロバイダ側処理装置 1 0 0 全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。

#### 【 0 0 2 3 】

磁気ディスク装置 2 0 3 は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置 2 0 4 は、利用者から受付けたアクセス内容の処理をアクセス処理装置 1 0 2 に要求する為の各種入力を行う装置である。

#### 【 0 0 2 4 】

出力装置 2 0 5 は、利用者から受付けたアクセス内容の処理要求に伴う各種出

力を行う装置である。CD-ROM装置206は、前記各種処理プログラムを記録したCD-ROMの内容を読み出す装置である。利用者属性DB207は、利用者の氏名、性別、年齢、職業、勤務先・役職等の各種属性を示す情報を格納するデータベースである。

## 【0025】

またプロバイダ側処理装置100は、利用者属性設定処理部210と、開示ポリシー処理部211と、アクセス要求処理部212とを有している。

## 【0026】

利用者属性設定処理部210は、利用者の各種属性を示す利用者属性を利用者側処理装置101から受信してプロバイダ側処理装置100内の利用者属性DB207に設定する処理部である。開示ポリシー処理部211は、利用者から要求されたアクセスの内容を示すアクセス内容と当該利用者の利用者属性の開示方針を示す利用者属性開示ポリシーとを利用者側処理装置101から受付け、当該アクセス内容の処理を実行するアクセス処理装置102とそのアクセス処理装置102に開示する利用者属性の内容とを前記利用者属性開示ポリシーに従って決定する処理部である。アクセス要求処理部212は、利用者側処理装置101から送信されたアクセス内容の処理を前記利用者属性の開示内容と共に前記決定したアクセス処理装置102に要求する処理部である。

## 【0027】

プロバイダ側処理装置100を利用者属性設定処理部210、開示ポリシー処理部211及びアクセス要求処理部212として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はCD-ROM以外の他の記録媒体でも良い。

## 【0028】

図3は本実施形態の利用者側処理装置101の概略構成を示す図である。図3に示す様に本実施形態の利用者側処理装置101は、CPU301と、メモリ302と、磁気ディスク装置303と、入力装置304と、出力装置305と、CD-ROM装置306とを有している。

【 0 0 2 9 】

CPU 3 0 1 は、利用者側処理装置 1 0 1 全体の動作を制御する装置である。  
メモリ 3 0 2 は、利用者側処理装置 1 0 1 全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。

【 0 0 3 0 】

磁気ディスク装置 3 0 3 は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置 3 0 4 は、利用者から入力されたアクセス内容の処理をプロバイダ側処理装置 1 0 0 に依頼する為の各種入力を行う装置である。

【 0 0 3 1 】

出力装置 3 0 5 は、利用者から入力されたアクセス内容の処理依頼に伴う各種出力を行う装置である。CD-ROM 装置 3 0 6 は、前記各種処理プログラムを記録した CD-ROM の内容を読み出す装置である。

【 0 0 3 2 】

また利用者側処理装置 1 0 1 は、利用者属性設定依頼処理部 3 1 0 と、アクセス依頼処理部 3 1 1 とを有している。

【 0 0 3 3 】

利用者属性設定依頼処理部 3 1 0 は、利用者側処理装置 1 0 1 を利用する利用者の各種属性を表す利用者属性の設定をプロバイダ側処理装置 1 0 0 に依頼する処理部である。アクセス依頼処理部 3 1 1 は、利用者から要求されたアクセスの内容を示すアクセス内容と当該利用者の利用者属性の開示方針を示す利用者属性開示ポリシーとを受付けて当該アクセス内容の処理をプロバイダ側処理装置 1 0 0 に依頼する処理部である。

【 0 0 3 4 】

利用者側処理装置 1 0 1 を利用者属性設定依頼処理部 3 1 0 及びアクセス依頼処理部 3 1 1 として機能させる為のプログラムは、CD-ROM 等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体は CD-ROM 以外の他の記録媒体でも良い。

【 0 0 3 5 】

図4は本実施形態のアクセス処理装置102の概略構成を示す図である。図4に示す様に本実施形態のアクセス処理装置102は、CPU401と、メモリ402と、磁気ディスク装置403と、入力装置404と、出力装置405と、CD-ROM装置406と、アクセス制御情報DB407とを有している。

【0036】

CPU401は、アクセス処理装置102全体の動作を制御する装置である。メモリ402は、アクセス処理装置102全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。

【0037】

磁気ディスク装置403は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置404は、プロバイダ側処理装置100から要求されたアクセス内容の処理を実行する為の各種入力を行う装置である。

【0038】

出力装置405は、プロバイダ側処理装置100から要求されたアクセス内容の処理実行に伴う各種出力を行う装置である。CD-ROM装置406は、前記各種処理プログラムを記録したCD-ROMの内容を読み出す装置である。アクセス制御情報DB407は、アクセス処理装置102でサイトを公開しているサイト公開者の各種属性や、利用者属性に応じたアクセス制御内容を示す情報を格納するデータベースである。

【0039】

またアクセス処理装置102は、アクセス制御情報設定処理部410と、アクセス実行処理部411とを有している。

【0040】

アクセス制御情報設定処理部410は、アクセス処理装置102でサイトを公開しているサイト公開者の各種属性や、利用者属性に応じたアクセス制御内容を示す情報をアクセス制御情報DB407に設定する処理部である。アクセス実行処理部411は、プロバイダ側処理装置100から要求されたアクセス内容の処理をそのアクセス内容と共に送られた利用者属性に対応する範囲内で実行する処理部である。

## 【0041】

アクセス処理装置102をアクセス制御情報設定処理部410及びアクセス実行処理部411として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はCD-ROM以外の他の記録媒体でも良い。

## 【0042】

本実施形態の利用者側処理装置101の利用者属性設定依頼処理部310は、利用者側処理装置101を利用する利用者の氏名、性別、年齢、職業、勤務先・役職等の利用者属性の設定をプロバイダ側処理装置100に依頼する処理を行い、プロバイダ側処理装置100の利用者属性設定処理部210は、前記利用者属性を利用者側処理装置101から受信してプロバイダ側処理装置100内の利用者属性DB207に設定する処理を行う。

## 【0043】

図5は本実施形態の利用者属性DB207の一例を示す図である。図5に示す様に本実施形態の利用者属性DB207には、利用者側処理装置101を利用する利用者の利用者属性として、氏名、性別、年齢、職業、勤務先・役職等の情報が格納されている。

## 【0044】

本実施形態のアクセス処理装置102のアクセス制御情報設定処理部410は、アクセス処理装置102でサイトを公開しているサイト公開者の各種属性や、利用者属性に応じたアクセス制御内容を示す情報をアクセス制御情報DB407に設定する処理を行う。

## 【0045】

図6は本実施形態のアクセス制御情報DB407の一例を示す図である。図6に示す様に本実施形態のアクセス制御情報DB407には、アクセス処理装置102でサイトを公開しているサイト公開者の属性として、サイト公開者名、サイト情報が格納され、プロバイダ側処理装置100からアクセス内容の処理を要求された場合にその利用者属性に応じたアクセス範囲を示すレベルを設定する為の

情報提供ポリシー、前記設定したレベルに応じた制御内容を示すアクセス制御情報が格納されている。ここで、サイト公開者名やサイト情報等の情報に第3者機関の認証情報を付加してその改竄を防止しているものとする。

#### 【0046】

この図6では、インフルエンザに関する情報検索を行う場合の情報提供ポリシー及びアクセス制御情報を示しており、他のアクセス内容について情報提供ポリシーを設定する場合にはその職業や役職の違いに応じて異なるアクセス制御レベルを設定し、またそれらのアクセス制御レベルに対応するアクセス制御情報にはアクセス制御レベルが高くなるに従ってより高度な情報へのアクセスが可能な制御情報が設定されるものとする。

#### 【0047】

以下に本実施形態のアクセス制御システムにおいて、利用者側処理装置101からアクセス内容の処理をプロバイダ側処理装置100に依頼し、当該アクセス内容の処理を実行するアクセス処理装置102とそのアクセス処理装置102に開示する利用者属性の内容とを利用者属性開示ポリシーに従って決定する処理をプロバイダ側処理装置100で行い、前記決定された開示内容の利用者属性に対応する範囲内で当該アクセス内容の処理をアクセス処理装置102で実行する処理について説明する。

#### 【0048】

図7は本実施形態のアクセス依頼処理の処理手順を示すフローチャートである。図7に示す様に利用者側処理装置101のアクセス依頼処理部311は、利用者から要求されたアクセスの内容を示すアクセス内容と当該利用者の利用者属性の開示方針を示す利用者属性開示ポリシーとを受付けて当該アクセス内容の処理をプロバイダ側処理装置100に依頼する処理を行う。

#### 【0049】

本実施形態のアクセス制御システムにおいて、利用者がインターネット等のネットワークで接続された各アクセス処理装置に対して情報検索等のアクセス内容の処理を要求する場合には、プロバイダ側処理装置100にログインしてそのネットワークに接続した後、そのアクセス内容と、その処理を実行する際に当該利

利用者の利用者属性をどれだけアクセス処理装置 1 0 2 へ開示するかを示す利用者属性開示ポリシーを利用者側処理装置 1 0 1 に入力する。

【 0 0 5 0 】

ステップ 7 0 1 で利用者側処理装置 1 0 1 のアクセス依頼処理部 3 1 1 は、プロバイダ側処理装置 1 0 0 にログインする為のユーザ ID 及びパスワードの入力を利用者から受付けてそれらの情報をプロバイダ側処理装置 1 0 0 へ送り、プロバイダ側処理装置 1 0 0 にログインする。

【 0 0 5 1 】

ステップ 7 0 2 では、利用者が要求するアクセス内容の入力が行われたかどうかを調べ、アクセス内容の入力が行われた場合にはステップ 7 0 3 へ進む。ステップ 7 0 3 では、前記入力されたアクセス内容を受付けてアクセス内容情報としてメモリ 3 0 2 に格納する。

【 0 0 5 2 】

ステップ 7 0 4 では、当該利用者の利用者属性の開示方針を示す利用者属性開示ポリシーの入力が行われたかどうかを調べ、利用者属性開示ポリシーの入力が行われた場合にはステップ 7 0 5 へ進む。ステップ 7 0 5 では、前記入力された利用者属性開示ポリシーを受付けて利用者属性開示ポリシー情報としてメモリ 3 0 2 に格納する。

【 0 0 5 3 】

ステップ 7 0 6 では、前記格納したアクセス内容情報及び利用者属性開示ポリシー情報をネットワーク経由でプロバイダ側処理装置 1 0 0 に送り、当該アクセス内容の処理をプロバイダ側処理装置 1 0 0 へ依頼する。

【 0 0 5 4 】

ステップ 7 0 7 では、前記依頼したアクセス内容の処理結果をプロバイダ側処理装置 1 0 0 から受信しているかどうかを調べ、アクセス内容の処理結果を受信している場合にはステップ 7 0 8 へ進む。ステップ 7 0 8 では、前記受信した処理結果を出力装置 3 0 5 へ表示する。

【 0 0 5 5 】

図 8 は本実施形態のアクセス要求処理の処理手順を示すフローチャートである

。図8に示す様にプロバイダ側処理装置100の開示ポリシー処理部211は、利用者から要求されたアクセスの内容を示すアクセス内容と当該利用者の利用者属性の開示方針を示す利用者属性開示ポリシーとを利用者側処理装置101から受付け、当該アクセス内容の処理を実行するアクセス処理装置102とそのアクセス処理装置102に開示する利用者属性の内容とを前記利用者属性開示ポリシーに従って決定する処理を行い、そしてアクセス要求処理部212は、利用者側処理装置101から送信されたアクセス内容の処理を前記利用者属性の開示内容と共に前記決定したアクセス処理装置102に要求する処理を行う。

【0056】

ステップ801でプロバイダ側処理装置100の開示ポリシー処理部211は、アクセス内容の処理依頼を利用者側処理装置101から受信しているかどうかを調べ、アクセス内容の処理依頼を受信している場合にはステップ802へ進む。

【0057】

ステップ802では、前記受信したアクセス内容の処理が可能なアクセス処理装置102からサイト情報を受信する。ステップ803では、利用者側処理装置101から受信した利用者属性開示ポリシーとアクセス処理装置102から受信したサイト情報とを比較して、そのアクセス処理装置102が利用者属性開示ポリシーで示された条件を満たしているかどうかを調べる認証処理を行い、利用者属性開示ポリシーの条件を満たしている場合にはステップ804へ進む。ステップ804では、利用者属性開示ポリシーの条件を満たしているアクセス処理装置102を当該アクセス内容の処理を実行する処理装置として設定する。

【0058】

ステップ805では、前記受信したアクセス内容の処理が可能な全てのアクセス処理装置102からサイト情報を受信したかどうかを調べ、またサイト情報を受信していないアクセス処理装置102がある場合にはステップ802へ戻り、全てのアクセス処理装置102からサイト情報を受信し終えた場合にはステップ806へ進む。

【0059】



なお本実施形態では前記の様に各アクセス処理装置102からサイト情報を受信して利用者属性開示ポリシーの条件を満たしているかどうかを判定しているが、予め各アクセス処理装置102からサイト情報を受信してプロバイダ側処理装置100に格納しておき、利用者側処理装置101から受信した利用者属性開示ポリシーとプロバイダ側処理装置100に格納されたサイト情報とを比較して、利用者属性開示ポリシーの条件を満たしているかどうかを判定しても良い。

#### 【0060】

ステップ806では、利用者側処理装置101から受信した利用者属性開示ポリシーに従って当該利用者のユーザIDに対応する利用者属性を利用者属性DB207から読み出して、アクセス処理装置102へ開示するマスキングされた利用者属性情報を設定する。

#### 【0061】

ステップ807でアクセス要求処理部212は、利用者側処理装置101から送信されたアクセス内容の処理を実行する処理装置として設定したアクセス処理装置102に当該アクセス内容及び前記マスキングされた利用者属性情報を送り、当該アクセス内容の処理を前記設定したアクセス処理装置102に要求する。

#### 【0062】

ステップ808では、前記要求したアクセス内容の処理結果をアクセス処理装置102から受信しているかどうかを調べ、アクセス内容の処理結果を受信している場合にはステップ809へ進む。ステップ809では、前記受信した処理結果を当該アクセス内容の処理を依頼した利用者側処理装置101へ送信する。

#### 【0063】

図9は本実施形態のアクセス実行処理の処理手順を示すフローチャートである。図9に示す様にアクセス処理装置102のアクセス実行処理部411は、プロバイダ側処理装置100から要求されたアクセス内容の処理をそのアクセス内容と共に送られた利用者属性に対応する範囲内で実行する処理を行う。

#### 【0064】

ステップ901でアクセス処理装置102のアクセス実行処理部411は、アクセス内容の処理要求をプロバイダ側処理装置100から受信しているかどうか

を調べ、アクセス内容の処理要求を受信している場合にはステップ902へ進む。

#### 【0065】

ステップ902では、プロバイダ側処理装置100から受信したマスキングされた利用者属性情報の内容とアクセス制御情報DB407中の情報提供ポリシーの内容とを比較してその利用者の利用者属性が情報提供ポリシーで示された条件を満たしているかどうかを調べる認証処理を行い、当該アクセス内容の処理を行う際のアクセス制御レベルを設定する。

#### 【0066】

ステップ903では、アクセス制御情報DB407中のアクセス制御情報の内容を参照し、前記設定したアクセス制御レベルの範囲内で当該アクセス内容の処理を実行する。ステップ904では、ステップ903でのアクセス内容の処理結果をプロバイダ側処理装置100へ送信する。

#### 【0067】

以下に本実施形態のアクセス制御システムにおいて、利用者側処理装置101からインフルエンザに関する情報検索の処理をプロバイダ側処理装置100に依頼し、当該情報検索を実行するアクセス処理装置102とそのアクセス処理装置102に開示する利用者属性の内容とを利用者属性開示ポリシーに従って決定する処理をプロバイダ側処理装置100で行い、前記決定された開示内容の利用者属性に対応する範囲内で当該情報検索をアクセス処理装置102で実行する処理について説明する。

#### 【0068】

図7のステップ701で利用者側処理装置101のアクセス依頼処理部311は、ユーザID及びパスワードを送信してプロバイダ側処理装置100にログインする。ステップ702では、利用者が要求するアクセス内容として、「インフルエンザにおいて可能な限り新しくかつ詳しい情報の検索」等の検索内容を入力し、ステップ703で検索内容情報としてメモリ302に格納する。ステップ704では、当該利用者の利用者属性の開示方針を示す利用者属性開示ポリシーとして図10に示す様な情報を入力し、ステップ705で利用者属性開示ポリシー

情報としてメモリ302に格納する。

【0069】

図10は本実施形態の利用者属性開示ポリシーの一例を示す図である。図10に示す様に本実施形態の利用者属性開示ポリシーでは、情報検索が行われるアクセス処理装置102の条件を示す情報として、サイト安全性・信頼性レベル「B」以上、プライバシー保護レベル「B」以上、大学、病院または医薬品企業のオフィシャルサイト、最終更新日時3ヶ月以内等が設定されており、そのアクセス処理装置102に対して開示する利用者属性情報の内容を示す情報として職業及び勤務先・役職が設定されている。

【0070】

ステップ706では、前記格納した検索内容情報及び利用者属性開示ポリシー情報をネットワーク経由でプロバイダ側処理装置100に送り、当該情報検索をプロバイダ側処理装置100へ依頼する。

【0071】

図8のステップ801でプロバイダ側処理装置100の開示ポリシー処理部211は、情報検索依頼を利用者側処理装置101から受信してステップ802へ進み、ステップ802では、その情報検索の実行が可能なアクセス処理装置102からサイト情報として、図6に示した様な(株)△□製薬オフィシャルサイト、サイト安全性・信頼性レベル「A」、プライバシー保護レベル「A」、最終更新日：〇〇〇〇年〇〇月〇〇日等の情報を受信する。

【0072】

ステップ803では、利用者側処理装置101から受信した利用者属性開示ポリシーのサイト安全性・信頼性レベル「B」以上、プライバシー保護レベル「B」以上、大学、病院または医薬品企業のオフィシャルサイト、最終更新日時3ヶ月以内等の情報と、アクセス処理装置102から受信したサイト情報の(株)△□製薬オフィシャルサイト、サイト安全性・信頼性レベル「A」、プライバシー保護レベル「A」、最終更新日：〇〇〇〇年〇〇月〇〇日等の情報とを比較して、そのアクセス処理装置102が利用者属性開示ポリシーで示された条件を満たしているかどうかを調べる認証処理を行い、ステップ804では、利用者属性開

示ポリシーの条件を満たしているアクセス処理装置102を当該情報検索の実行を行う処理装置として設定する。

【0073】

ステップ805では、前記情報検索の実行が可能な全てのアクセス処理装置102からサイト情報を受信したかどうかを調べ、全てのアクセス処理装置102からサイト情報を受信し終えた場合にはステップ806へ進む。

【0074】

ステップ806では、利用者側処理装置101から受信した利用者属性開示ポリシーに従って当該利用者のユーザIDに対応する職業「医師」及び勤務先・役職「〇×病院院長」の情報を利用者属性DB207から読み出して、アクセス処理装置102へ開示するマスキングされた利用者属性情報を設定する。

【0075】

ステップ807でアクセス要求処理部212は、前記情報検索を実行する処理装置として設定したアクセス処理装置102に当該検索内容及び前記マスキングされた利用者属性情報を送り、当該情報検索を前記設定したアクセス処理装置102に要求する。

【0076】

ステップ901でアクセス処理装置102のアクセス実行処理部411は、情報検索要求をプロバイダ側処理装置100から受信してステップ902へ進む。ステップ902では、プロバイダ側処理装置100から受信したマスキングされた利用者属性情報の内容である職業「医師」及び勤務先・役職「〇×病院院長」と、アクセス制御情報DB407中の情報提供ポリシーの内容とを比較してその利用者の利用者属性が情報提供ポリシーで示された条件を満たしているかどうかを調べる認証処理を行い、当該情報検索を行う際のアクセス制御レベルとしてレベル「A」を設定する。

【0077】

ステップ903では、アクセス制御情報DB407中のアクセス制御情報の内容を参照し、前記設定したレベル「A」の範囲内で情報検索処理を行う。すなわちレベル「A」では最新研究成果のアクセスが許されており、その最新研究成果

の情報が格納されたデータベースを検索する。ここで、レベル「A」の範囲内ではそれ以下の情報にもアクセス可能であるものとし、レベル「B」の最新ウィルス種別及び対応ワクチンの情報が格納されたデータベース及びレベル「C」のインフルエンザについての情報が格納されたデータベースも検索するものとしても良い。ステップ904では、ステップ903での情報検索結果をプロバイダ側処理装置100へ送信する。

## 【0078】

ステップ808でプロバイダ側処理装置100のアクセス要求処理部212は、前記の様に利用者属性に応じた最新研究成果を含む情報検索結果を受信し、ステップ809では当該情報検索を依頼した利用者側処理装置101へその情報検索結果を送信する。ステップ707で利用者側処理装置101のアクセス依頼処理部311は、当該利用者の利用者属性に応じた最新研究成果を含む情報検索結果を受信し、ステップ708でその情報検索結果を出力装置305へ表示する。

## 【0079】

前記の様に本実施形態では、利用者の属性情報に応じてアクセス内容进行处理するので、多くの利用者のユーザ管理に伴うアクセス処理装置102側での負担やリスクを増やすことなく、利用者毎に木目細かなアクセス制御を行うことが可能である。

## 【0080】

また本実施形態では、利用者属性の開示内容及び開示先を利用者属性開示ポリシーに従って制限しているので、利用者のプライバシーを保護することが可能である。更に本実施形態では、そのアクセス処理装置102が利用者属性開示ポリシーで示された条件を満たしているかどうかを調べる認証処理と、その利用者の利用者属性が情報提供ポリシーで示された条件を満たしているかどうかを調べる認証処理、すなわち利用者側のポリシーによる認証処理とアクセス処理装置102側のポリシーによる認証処理という双方向の認証処理を行っている為、より高度なアクセス制御を行うことが可能である。

## 【0081】

また本実施形態では、各装置間で送受信される情報のインタフェースを統一し

、自動的に情報を要求・提供するエージェント技術に適用して、双方向認証、情報の要求／提供等の各種アクセス処理をエージェントによって実行することにより、木目細かな制御の完全な自動化を行うことが可能である。

【 0 0 8 2 】

以上説明した様に本実施形態のアクセス制御システムによれば、利用者から要求されたアクセス内容の実行を当該利用者の利用者属性に応じて制御するので、要求されたアクセス内容の実行側での利用者管理等の負担を増やすことなく利用者毎に木目細かなアクセス制御を行うことが可能である。

【 0 0 8 3 】

【発明の効果】

本発明によれば利用者から要求されたアクセス内容の実行を当該利用者の利用者属性に応じて制御するので、要求されたアクセス内容の実行側での利用者管理等の負担を増やすことなく利用者毎に木目細かなアクセス制御を行うことが可能である。

【図面の簡単な説明】

【図 1】

本実施形態のアクセス制御システムの概略構成を示す図である。

【図 2】

本実施形態のプロバイダ側処理装置 1 0 0 の概略構成を示す図である。

【図 3】

本実施形態の利用者側処理装置 1 0 1 の概略構成を示す図である。

【図 4】

本実施形態のアクセス処理装置 1 0 2 の概略構成を示す図である。

【図 5】

本実施形態の利用者属性 DB 2 0 7 の一例を示す図である。

【図 6】

本実施形態のアクセス制御情報 DB 4 0 7 の一例を示す図である。

【図 7】

本実施形態のアクセス依頼処理の処理手順を示すフローチャートである。

【図 8】

本実施形態のアクセス要求処理の処理手順を示すフローチャートである。

【図 9】

本実施形態のアクセス実行処理の処理手順を示すフローチャートである。

【図 1 0】

本実施形態の利用者属性開示ポリシーの一例を示す図である。

【符号の説明】

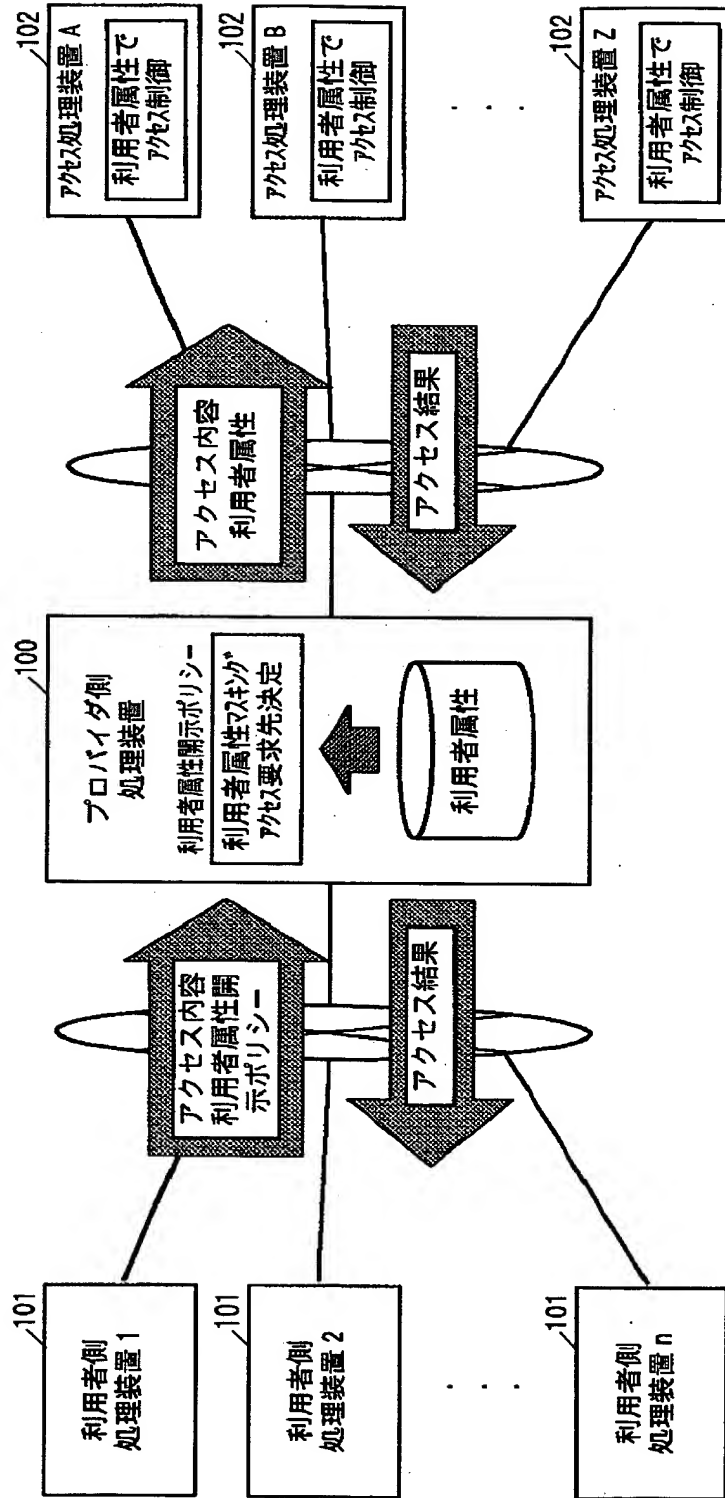
1 0 0 …プロバイダ側処理装置、1 0 1 …利用者側処理装置、1 0 2 …アクセス処理装置、2 0 1 …CPU、2 0 2 …メモリ、2 0 3 …磁気ディスク装置、2 0 4 …入力装置、2 0 5 …出力装置、2 0 6 …CD-ROM装置、2 0 7 …利用者属性DB、2 1 0 …利用者属性設定処理部、2 1 1 …開示ポリシー処理部、2 1 2 …アクセス要求処理部、3 0 1 …CPU、3 0 2 …メモリ、3 0 3 …磁気ディスク装置、3 0 4 …入力装置、3 0 5 …出力装置、3 0 6 …CD-ROM装置、3 1 0 …利用者属性設定依頼処理部、3 1 1 …アクセス依頼処理部、4 0 1 …CPU、4 0 2 …メモリ、4 0 3 …磁気ディスク装置、4 0 4 …入力装置、4 0 5 …出力装置、4 0 6 …CD-ROM装置、4 0 7 …アクセス制御情報DB、4 1 0 …アクセス制御情報設定処理部、4 1 1 …アクセス実行処理部。

【書類名】

図面

【図 1】

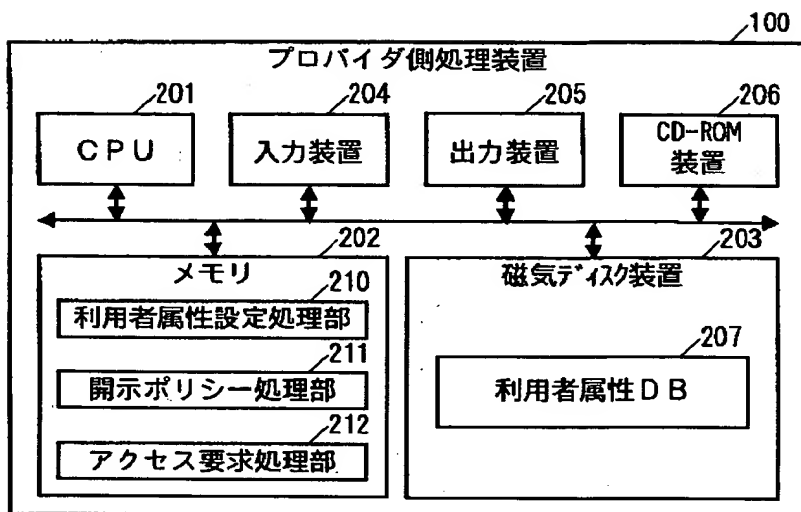
図 1





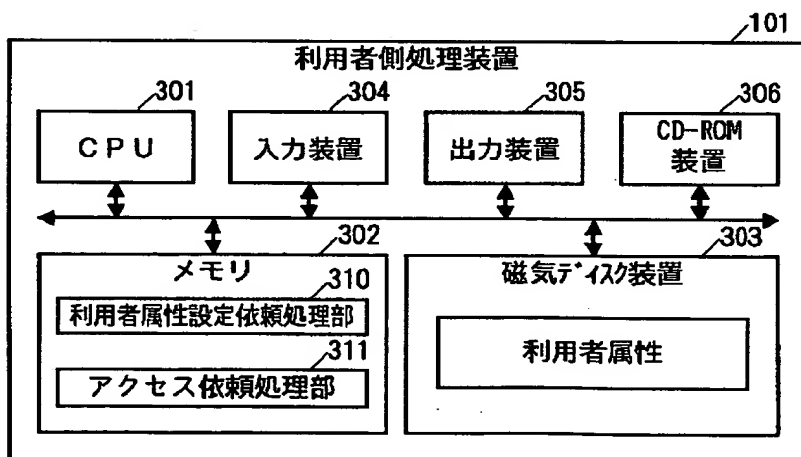
【図 2】

図 2



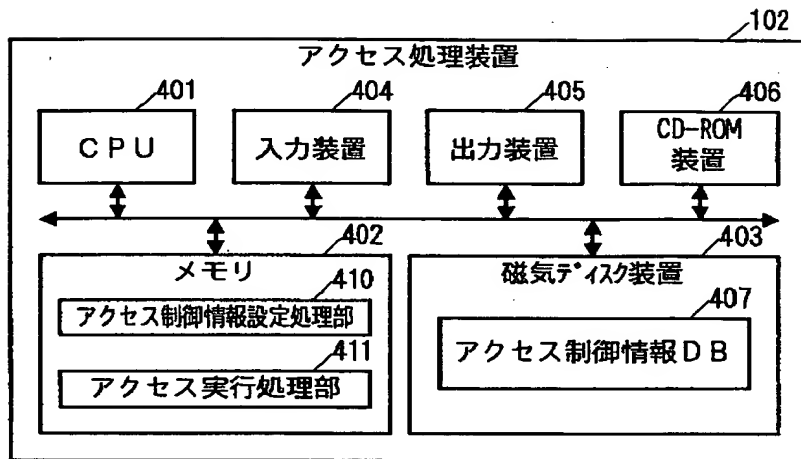
【図 3】

図 3



【図 4】

図 4



【図 5】

図 5

207

ユーザID	氏名	性別	年齢	職業	勤務先・役職	:
0001	日立太郎	男	55	医師	○×医院院長	:
0002	日立花子	女	39	会社員	○□会社研究員	:
0003	鈴木三郎	男	28	会社員	△□製薬	:
:	:	:	:	:	:	:

【図6】

図6

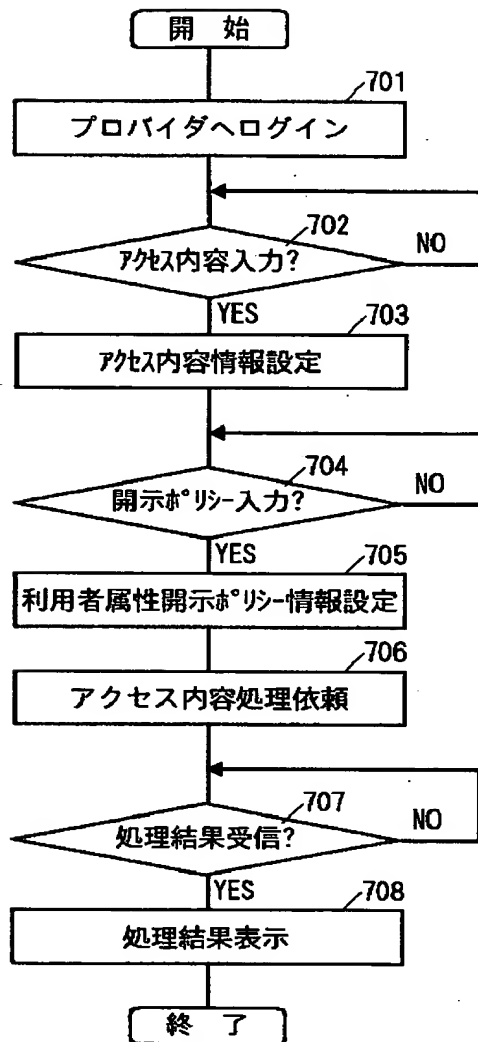
アクセス制御情報のデータ構造

407

項番	項目名	内容
1	サイト公開者	(株)△□製薬
2	サイト情報	<ul style="list-style-type: none"> <li>・ (株)△□製薬オフィシャルサイト</li> <li>・ サイト安全性・信頼性レベル「A」</li> <li>・ プライバシー保護レベル「A」</li> <li>・ 最終更新日：〇〇〇〇年〇〇月〇〇日</li> </ul>
3	情報提供ポリシー	レベル「A」：利用者属性の役職が「院長」 レベル「B」：利用者属性の職業が「医師」 レベル「C」：利用者属性の職業が「医師」以外 レベル「D」：利用者属性の提供無し
4	アクセス制御情報	レベル「A」：最新研究成果 レベル「B」：最新ウィルス種別、対応ワクチン レベル「C」：インフルエンザについて レベル「D」：アクセス不可

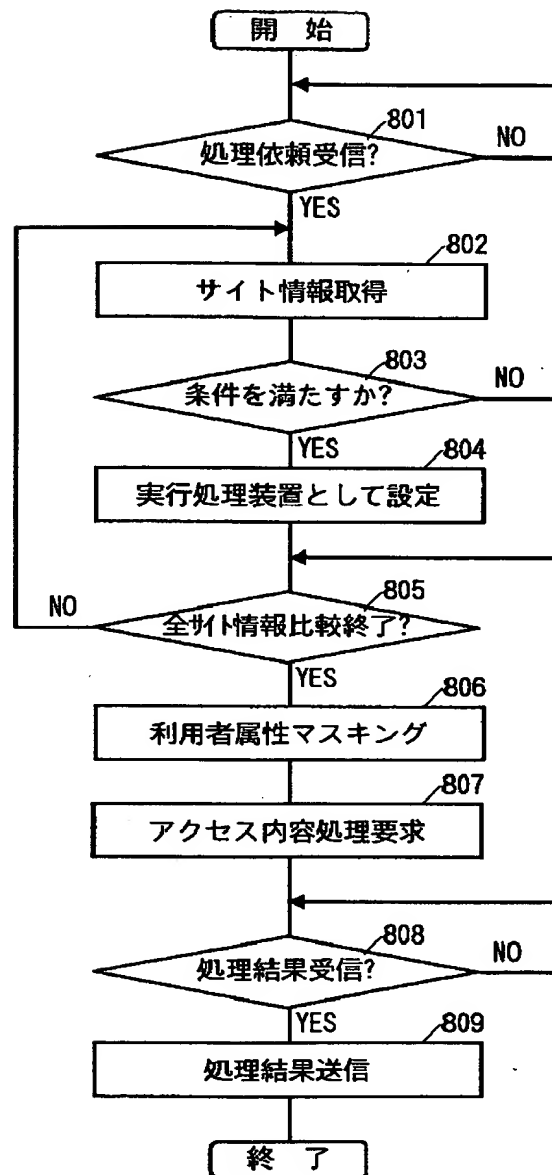
【図 7】

図 7

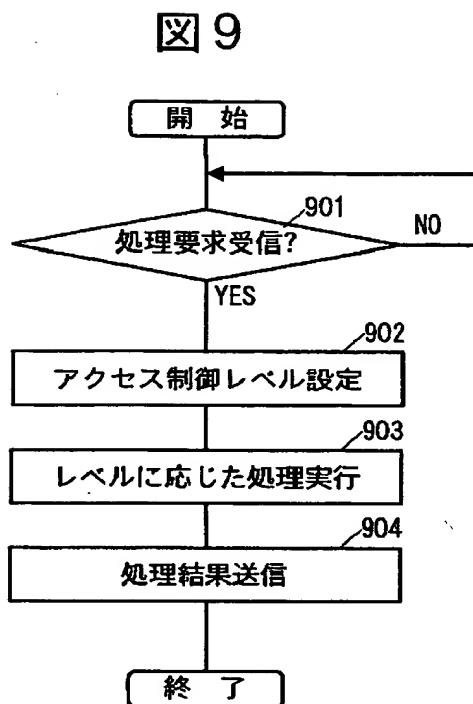


【図 8】

図 8



【図 9】



【図 1 0】

**図 1 0**

利用者属性 開示ポリシー	<b>アクセス処理装置の条件</b> 以下のすべてを満たすもの <ul style="list-style-type: none"> <li>・ サイト安全性・信頼性レベル「B」以上</li> <li>・ プライバシー保護レベル「B」以上</li> <li>・ 大学、病院または医薬品企業のオフィシャルサイトに限る</li> <li>・ 最終更新日時3ヶ月以内</li> </ul>
	<b>利用者属性開示内容</b> 職業 勤務先・役職

【書類名】 要約書

【要約】

【課題】 要求されたアクセス内容の実行側での利用者管理等の負担を増やすことなく利用者毎に木目細かなアクセス制御を行うことが可能な技術を提供する。

【解決手段】 利用者から受付けたアクセス内容の実行を制御するアクセス制御方法において、利用者から要求されたアクセスの内容を示すアクセス内容を受付けるステップと、前記受付けたアクセス内容の実行を当該利用者の利用者属性と共に要求するステップと、前記要求されたアクセス内容の処理をそのアクセス内容と共に送られた利用者属性に対応する範囲内で実行するステップとを有するものである。

【選択図】 図 1

特2000-297937

認定・付加情報

特許出願の番号	特願2000-297937
受付番号	50001260928
書類名	特許願
担当官	第七担当上席 0096
作成日	平成12年10月 3日

<認定情報・付加情報>

【提出日】	平成12年 9月29日
-------	-------------

次頁無



出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日	1990年 8月31日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台4丁目6番地
氏 名	株式会社日立製作所